

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-051948

(43)Date of publication of application : 23.02.2001

(51)Int.Cl.

G06F 15/00

H04L 9/32

H04L 12/46

H04L 12/28

H04L 12/22

(21)Application number : 11-229671

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 16.08.1999

(72)Inventor : MITSUFUJI TAKASHI

NIKI TERUNORI

ISHIKAWA AKIRA

HINO TETSUYA

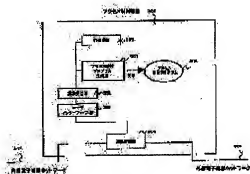
UEDA MAOMI

(54) DEVICE AND SYSTEM FOR ACCESS CONTROL

(57)Abstract:

PROBLEM TO BE SOLVED: To permit access without lowering the security level by generating an accepting program only when the access request from electronic equipment on an external network meet specific access permission conditions.

SOLUTION: When the contents and conditions of access permission are specified in an operation screen of a user interface(UIF) part 303, a request acceptance part 302 to which the specification contents have been transmitted generates an ID and a password(PW) needed for access by an ID generation part 305 to obtain them. Then the request acceptance part 302 makes an access accepting program generation part 301 generate an access accepting program and embeds the generated ID and PW in the program 306. A program generation part 301 starts the program 301 to inform the UIF part 303 of an access acceptance address through the request acceptance part 302 to display the ID and PW and the access acceptance address of the access accepting program on the screen of a television set, thereby informing a user who is allowed to permit access.



LEGAL STATUS

[Date of request for examination]	10.07.2001
[Date of sending the examiner's decision of rejection]	14.06.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-51948

(P2001-51948A)

(43) 公開日 平成13年2月23日 (2001.2.23)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 C 5 B 0 8 5
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A 5 J 1 0 4
12/46		11/00	3 1 0 C 5 K 0 3 0
12/28		11/26	5 K 0 3 3
12/22			9 A 0 0 1
審査請求 未請求 請求項の数10 O L (全 30 頁)			
(21) 出願番号	特願平11-229671	(71) 出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22) 出願日	平成11年8月16日 (1999.8.16)	(72) 発明者	三藤 隆 大阪府門真市大字門真1006番地 松下電器産業株式会社内
		(73) 発明者	仁木 輝記 大阪府門真市大字門真1006番地 松下電器産業株式会社内
		(74) 代理人	100097445 弁理士: 岩橋 文雄 (外 2 名)

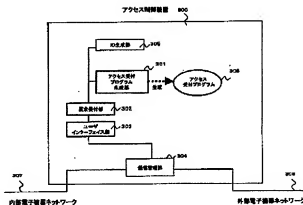
最終頁に続く

(54) 【発明の名称】 アクセス制御装置及びアクセス制御システム

(57) 【要約】

【課題】 電子機器ネットワーク上の機器やサービスに対する外部ネットワークからのアクセスを、必要になった時点で、必要なアクセス内容に対してのみ、必要なアクセス許可条件のもとで、セキュリティレベルを下げずに、許可する事を可能とするアクセス制御装置、及びアクセス制御システムを提供する。

【解決手段】 電子機器ネットワークにおいて、該電子機器ネットワークのユーザが指定したアクセス許可条件を満たす場合に限り、異なる管理下にある外部電子機器ネットワーク上の電子機器、又はサービスから該ユーザが指定したアクセス許可内容へのアクセスを受け付け、中継することにより、アクセス先にアクセスするアクセス受付プログラムを、該電子機器ネットワークのユーザからの要求に応じて生成する。



【特許請求の範囲】

【請求項1】 電子機器を接続した内部電子機器ネットワークに、外部の電子機器ネットワーク上の電子機器からアクセス要求がされるアクセス制御装置であって、外部電子機器ネットワーク上の電子機器から内部電子機器ネットワーク内へのアクセス要求が、特定のアクセス許可条件を満たし、かつ、アクセスを許可した特定のアクセス許可内容に対するアクセス要求である場合に限り、そのアクセス要求を受け付け、要求されたアクセス先との間の許可したアクセス許可内容の通信を中継するアクセス受付プログラム、の生成要求を受け付ける要求受付手段と、前記生成要求に応じたアクセス受付プログラムの生成を行うアクセス受付プログラム生成手段と、を有することを特徴とするアクセス制御装置。

【請求項2】 あらかじめ設定された条件にしたがってアクセス受付プログラムの起動及び終了の少なくとも一方を行うことが可能であるアクセス受付プログラム管理手段を有することを特徴とする請求項1に記載のアクセス制御装置。

【請求項3】 前記アクセス受付プログラム管理手段は、前記指定されたアクセス許可条件から判断してアクセス要求の受付をしてもよい期間の間だけそのアクセス許可条件に対応するアクセス受付プログラムの代わりに、そのアクセス受付プログラムへのアクセスを待ち、アクセスが発生した時にそのアクセス受付プログラムを起動しそのアクセス受付プログラムに処理を移行することを特徴とする請求項1に記載のアクセス制御装置。

【請求項4】 前記アクセス要求を受け付けて、少なくともアクセス先の電子機器との通信のアクセス制御を行う特定のアクセス受付プログラムにアクセスし、前記電子機器ネットワーク上の電子機器と通信するプログラムであるアクセスクライアントプログラムの生成要求を受け付ける要求受付手段と、前記生成要求に応じたアクセスクライアントプログラムの生成を行うアクセスクライアントプログラム生成手段と、を有することを特徴とするアクセス制御装置。

【請求項5】 前記アクセス要求を受け付けて、少なくともアクセス先の電子機器との通信のアクセス制御を行う特定のアクセス受付プログラムにアクセスし、前記アクセスを行うために必要な情報を含むデータであるアクセスチケットの生成要求を受け付ける要求受付手段と、前記生成要求に応じたアクセスチケットの生成を行うアクセスチケット生成手段と、を有することを特徴とするアクセス制御装置。

【請求項6】 前記アクセスクライアントプログラム生成手段は、アクセス受付プログラムとの通信の際に通信内容を暗号化及び復号化するための暗号鍵データを内部に含むアクセスクライアントプログラムを生成すること

【請求項7】 前記アクセスチケット生成手段は、アクセス受付プログラムとの通信の際に通信内容を暗号化及び復号化するための暗号鍵データを内部に含むアクセスチケットを生成することを特徴とする請求項5に記載のアクセス制御装置。

【請求項8】 指定されたアクセス制御情報、アクセス受付プログラム、アクセスクライアントプログラム、アクセスチケットのいずれかが存在する場合に、それらを削除する削除手段を有することを特徴とする請求項1に記載のアクセス制御装置。

【請求項9】 前記アクセス受付プログラムの生成を行うアクセス受付プログラム生成手段と、前記アクセスクライアントプログラムの生成を行うアクセスクライアントプログラム生成手段と、生成したアクセスクライアントプログラムを別の電子機器へ転送するデータ送信手段と、を有することを特徴とするアクセス制御装置と、アクセスクライアントプログラムを受信するデータ受信手段を有する電子機器と、を備え、前記アクセス制御装置から電子機器へアクセスクライアントプログラムを転送し、そのアクセスクライアントプログラムを用いることによりアクセス受付プログラムにアクセスすることを特徴とするアクセス制御システム。

【請求項10】 前記アクセス受付プログラムの生成を行うアクセス受付プログラム生成手段と、前記アクセスチケットの生成を行うアクセスチケット生成手段と、生成したアクセスチケットを別の電子機器へ転送するデータ送信手段と、を有することを特徴とするアクセス制御装置と、アクセスチケットを受信するデータ受信手段を有する電子機器と、を備え、前記アクセス制御装置から電子機器へアクセスチケットを転送し、そのアクセスチケットに含まれる情報を用いることによりアクセス受付プログラムにアクセスすることを特徴とするアクセス制御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数の電子機器ネットワーク間にまたがるアクセスを制御するアクセス制御装置、及びアクセス制御システムに関し、特に、ある1つの電子機器ネットワークの外部から内部へのアクセスに対する、柔軟かつ動的なアクセス制御を可能とするアクセス制御装置及びアクセス制御システムに関するものである。

【0002】

【従来の技術】近年、インターネットの利用者は急激に増加している。又、企業では計算機やプリンタなどの電子機器回線と、LAN（ローカルエリアネットワーク）

く)が普及している。

【0003】一方、家庭内の電子機器同士をネットワークで接続し、相互にサービスを利用し合うホームネットワークの普及も始まっている。ホームネットワークと外部のインターネットとを接続することにより、インターネットを利用した家庭向けの有益なサービスが実現可能となる。しかし、それと同時に、ネットワーク犯罪やプライバシーの侵害といったセキュリティの問題が大きな課題となっている。

【0004】例えば、部外者に外部ネットワークからホームネットワークに侵入されて、個人の大切なデータを盗まれたり、消去されたり、家庭内の電子機器を不当に操作されてしまったりすることが考えられる。

【0005】従来、電子機器ネットワークの外部から内部へのアクセスに対するアクセス制御を行う方法としては、主に企業内LANに対する外部のインターネットからの不正アクセスを防止するファイアウォール技術の一形態である「アプリケーションレベルプロキシ」があった。アプリケーションレベルプロキシとは、内部ネットワークのユーザ、又はサービスと、インターネットなどの外部ネットワーク上のユーザ、又はサービスとの間の通信を、直接ではなく、両ネットワークの境界に位置する計算機上で動作させたプロキシ（代理人の意味）と呼ばれる中継プログラムを経由して行う手法である。これにより、両者間で通信するデータをそのまま素通りさせずに、プロキシが一旦データを代理で受け取り、管理者により前もってアクセスを許可された内容のアクセスであるかを調べ、アクセスが許可された場合にのみ、要求された通信先に転送することにより、不正アクセスを防止するというものである。

【0006】この他には、例えば、特開平8-153072号公報では、計算機ネットワークにおいて、ある計算機のあるユーザからの別のある計算機へのアクセスを許可するかどうかを判断するための、アクセス許可内容とアクセス許可条件を含むアクセス許可情報を、ユーザからの要求によって生成し、それを保持し、それをもとに実際にアクセスされた時にアクセスを許可するかどうかを判断する、というシステムについて開示されている。この公報の中では、アクセス元の計算機が別の計算機ネットワーク上にある場合についても触れられており、その場合のシステムのアクセス制御の仕組みの構成図を本発明と対比しやすいように描いたものが図23に示すブロック図である。この図の中で、2501は、内部ネットワーク上のユーザから、外部計算機ネットワーク上の計算機からの内部計算機ネットワーク上の計算機に対するアクセスを許可することの要求を受け付ける要求受付手段、2502は、ユーザから要求を受けたアクセス許可内容とアクセス許可条件を保持するアクセス制御情報保存手段、2503は、外部からのアクセス要求があった場合に、アクセスを許可するかどうかを、上記アクセス制御情報

報保存部に保持しているアクセス制御情報をもとに判断し、許可する場合には、通信を中継するアクセス受付プログラム、2504は、ネットワークを通じての通信を行う通信管理手段、2505は、ユーザの所属する計算機ネットワーク、2506は、異なる管理下にある計算機ネットワークである。

【0007】処理の流れは以下になる。

【0008】ユーザから外部計算機ネットワーク2505上の計算機からのアクセスの許可要求を受けた要求受付手段2501は、アクセス制御情報保存手段2502にユーザから要求を受けたアクセス許可内容とアクセス許可条件を保存する。そして、あらかじめ用意されていたアクセス受付プログラム2503は、外部計算機ネットワーク2505上の計算機から内部計算機ネットワーク上の計算機宛に対するアクセスがあった場合にそれを検知し、アクセス制御情報保存手段2502に保存してあるアクセス許可内容とアクセス許可条件を参照し、アクセスを許可すると判断した場合にのみ、通信データをアクセス先計算機に転送することにより、内部計算機ネットワーク上の計算機へのアクセスを実現する。

【0009】この方法では、上記のアプリケーションレベルプロキシの場合と比べると、ユーザがアクセス許可条件、及びアクセス許可内容を必要に応じて設定出来るという点で、改善されている。

【0010】

【発明が解決しようとする課題】しかしながら、このような従来技術では、最終的なアクセスは拒否される可能性があるとしても、アクセス要求自体は常時受け付けられるため、そのアクセス要求受付の入り口が悪意を持ったユーザからの不正アクセスを許してしまう可能性があるという問題がある。これは、たとえ、アクセスを許可する期間が定められたとしても同様である。又、上記特開平8-153072号公報では、アクセス要求を受けた時、アクセスを許可する場合にのみ、対応するアクセス受付プログラムを起動する方法についても開示されているが、この場合でも、アクセス要求をある固定的なアクセス受付アドレスで、常時受け付けることになるため、同様にセキュリティ面で問題がある。

【0011】又、ホームネットワークを考えた場合には、企業内のLANの場合とは異なり、利用する電子機器の種類とそれらを用いたサービスの種類が多く、しかもこれらの種類は随時増えていく。そして、これらのホームネットワーク内部の種々の電子機器、又はサービスへの、外部ネットワーク上のある特定の部外者からの一時的なアクセスを受け入れる必要性が高い。例えば、ホームネットワークに接続された電子機器の遠隔保守サービスを実現する場合、保守が必要になった時点で、遠隔保守のためにその電子機器の操作を行う間、その電子機器に対してのみ、保守サービス業者による一時的なアクセスを許可する必要があると望ましい。

受付プログラムの生成を行うアクセス受付プログラム生成手段と、を有するものである。

電子機器又はサービスに対するアクセス要求を受け付け、アクセス制御を行う特定のアクセス受付プログラムにアクセスし、通信することを通じて、前記内部電子機器ネットワーク上の電子機器と通信するプログラムであるアクセスクライアントプログラムの生成要求を受け付ける要求受付手段と、該要求に応じたアクセスクライアントプログラムの生成を行うアクセスクライアントプログラム生成手段と、を有するものである。

【0024】これにより、アクセス受付プログラムが、アクセスクライアントプログラムからのアクセスのみを受け付けようとして、アクセスクライアントプログラムを保持している者だけがアクセス受付プログラムにアクセス可能であるようにすることが可能となり、そうすることによってセキュリティが大きく向上する。又、アクセスクライアントプログラムにGUI（グラフィカルユーザインターフェイス。画面に表示したボタンやメニューなどを操作するユーザインターフェイス。）を装備することにより、利用者がアクセスに必要な操作を、GUIを通して容易に行うことを可能とし、又、同時に、許可された内容以外への操作が出来ないように操作可能な範囲を限定し、かつ、操作可能範囲を、操作するユーザが認知することが可能となる。

【0025】第5に、本発明は、外部電子機器ネットワーク上の電子機器からの内部電子機器ネットワーク上の電子機器に対するアクセス要求を受け付け、アクセス制御を行う特定のアクセス受付プログラムにアクセスし、通信することを通じて、前記電子機器ネットワーク上の電子機器に対してアクセスを行うために必要な情報を含むデータであるアクセスチケット、の生成要求を受け付ける要求受付手段と、該要求に応じたアクセスチケットの生成を行うアクセスチケット生成手段と、を有するものである。

【0026】これにより、アクセスチケットを保持している者だけに対してアクセス受付プログラムへのアクセスを許可することが可能となり、セキュリティが大きく向上する。又、アクセスクライアントプログラムと比較すると、アクセスチケットはデータサイズが少なく済み、電子機器において持ち運ぶ際に、より小さな記憶領域に格納できる上、ネットワークを介しての転送時間も短くてすむという効果が得られる。アクセスチケットと引き換えにアクセスクライアントプログラムを取得するようにすれば、両者のメリットを活かすことも容易に可能である。

【0027】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態について説明する。

【0028】まず最初に、本発明の実施の形態において基本となる第1の実施の形態を説明し、続いてそれを応用したシステムの実施の形態を説明する。

【0029】なお、本発明（本発明の実施の形態）に何ら

限定されるものではなく、その趣旨を逸脱しない範囲において、種々なる態様で実施し得る。

【0030】（第1の実施の形態）まず、本発明の第1の実施の形態について説明する。

【0031】図1は、本実施の形態のアクセス制御システムの全体構成を表したものであり、この図において、101は、アクセス制御装置であり、本実施の形態では、外部ネットワークと内部ネットワークの境界上に位置し、内部ネットワークと外部ネットワークを接続するゲートウェイ装置の機能も兼ねることとする。102は、ユーザとのやり取りを行うための操作画面を表示する役割を果たすモニター装置であり、本実施の形態では、ホームネットワーク機能を持ったテレビであるとする。103は、外部電子機器ネットワークからアクセスされる対象となる電子機器であり、本実施の形態では、ホームネットワークに接続された電子機器であり、例えば、エアコン、洗濯機、オーディオ機器などの家庭電化製品や各種センサーなどあらゆる電子機器が考えられるが、ここでは、エアコンであるとする。104は、前記電子機器を接続する電子機器ネットワークで、本実施の形態では、TCP/IPプロトコルを使用した家庭内のホームネットワークであるとする。105は、広域電子機器ネットワーク網であり、本実施の形態では、インターネットとその先につながる種々のネットワーク全体であることとする。106は、外部電子機器ネットワークに接続された、内部電子機器ネットワークへアクセスするために使用するアクセス装置であり、本実施の形態では、エアコンのメンテナンスサービスを行うサービス会社内のインターネットに接続されたパーソナルコンピュータであるとする。

【0032】なお、本実施の形態では、ホームネットワークを「内側」のネットワーク、インターネットとその先につながる種々のネットワーク全体を「外側」のネットワークと考える。

【0033】本実施の形態では、最終的に、メンテナンスサービスを行うサービス会社内のパーソナルコンピュータから、アクセス制御装置を通じて、エアコンにアクセスすることを実現する。（図2参照）そのための手順の概要は以下のようなになる。

【0034】手順1：ユーザがテレビ画面を通して、アクセス制御装置101を操作し、外部電子機器ネットワーク105からのエアコンへの一時的なアクセス許可を要求する。

【0035】手順2：アクセス制御装置101が、アクセス要求内容に応じたアクセス受付プログラムを生成し、それに伴って、アクセスに使用するIDとパスワードを生成し、アクセス受付プログラムのアクセス受付アドレスとそのIDとパスワードをユーザに転送する。

【0036】手順3：ユーザがアクセスを許可する相手（エアコン（メンテナンスサービスの担当者））に何らかの

方法、例えば、電話や電子メールなどを使って、アクセス受付アドレスと生成した一時アクセス用のIDとパスワードを通知する。

【0037】手順4：通知を受けたユーザが、通知されたアクセス受付アドレスでアクセス受付をしているアクセス受付プログラムにアクセスし、IDとパスワードを入力しアクセス許可を得て、アクセス受付プログラム経由でエアコンにアクセスする。

【0038】以下、本実施の形態における各電子機器装置の構成についてを説明する。

【0039】図3は、本実施の形態でのアクセス制御装置の構成であり、301は、アクセス受付プログラムを生成するアクセス受付プログラム生成部、302は、ユーザからのアクセス制御の要求を受け付ける要求受付部、303は、モニター装置を通してユーザとのやり取りを行うユーザインターフェイス部、304は、ネットワークを通じての通信を行う通信管理部、305は、アクセス許可対象者がアクセス時に使用するIDとパスワードを生成するID生成部、306は、アクセス受付プログラム生成部によって生成されたアクセス受付プログラム、を示している。307は、電子機器を接続した内部電子機器ネットワークで、本実施の形態では、TCP/IPプロトコルを使用した家庭内のホームネットワークであり、308は、外部（広域）電子機器ネットワークであり、本実施の形態では、インターネットであるとする。

【0040】図4は、本実施の形態で、外部電子機器ネットワークからのアクセス対象となる内部電子機器ネットワークに接続された電子機器の構成図であり、401は、電子機器外部からの操作命令を受け付け、実行するサービスプログラム、402は、電子機器ネットワーク403を通じての通信を行う通信管理部、を示している。

【0041】図5は、モニター装置の構成図であり、501は、ユーザの操作を受け付け、その結果を表示するユーザインターフェイス部、502は、電子機器ネットワーク上のサービスを呼び出し、利用するサービス呼出部、503は、電子機器ネットワーク504を通じての通信を行う通信管理部、を示している。

【0042】図6は、外部電子機器ネットワークに接続された、内部電子機器ネットワークへアクセスするために使用するアクセス装置の構成図であり、601は、プログラムを実行するプログラム実行部、602は、電子機器ネットワーク603を通じての通信を行う通信管理部、を示している。本実施の形態では、プログラム実行部は、WWWサービスの利用を可能にするWebブラウザであるとする。

【0043】以下、実際の処理の流れを順に説明していく。更に詳細の処理内容の説明が必要な部分について

【0044】図7は、アクセス受付プログラム生成までの処理の流れを示したものである。縦の線が各構成要素を示し、矢印が通信やデータの流れを示しており、上から下へ処理は流れていくことを示しているものである。以下、図に沿って順に説明していく。

【0045】処理A-1：ホームネットワークのユーザ（その家の住人のAさん）がテレビの画面でリモコンなど操作して、サービス呼び出し部（図5の502）の操作画面を表示し、操作することによりアクセス制御装置300（図3）のユーザインターフェイス部303を呼び出し、その操作画面を表示する。

【0046】処理A-2：アクセス制御装置300のユーザインターフェイス部303の操作画面で、アクセス許可内容とアクセス許可条件を指定する。ここでは例えば、「2010年5月24日12時から14時までの間だけ、エアコンの保守コマンドのみをIDとパスワードを知るユーザが実行できるようにする」という内容を指定したものであるとして説明を進める。

【0047】処理A-3：ユーザインターフェイス部303はユーザから指定された内容を要求受付部302に伝達する。

【0048】処理A-4：要求受付部302は、次に、ID生成部305にアクセスに必要なIDとパスワードの生成要求を出す。

【0049】処理A-5：生成要求を受けたID生成部305は一時アクセス用のIDとパスワードを生成する。

【0050】処理A-6：ID生成部305は、生成したIDとパスワードを要求受付部302に通知する。

【0051】処理A-7：要求受付部302は、アクセス受付プログラム生成部301にアクセス受付プログラム306の生成要求を出す。この時に、生成されたIDとパスワードを通知することにより、アクセス受付プログラム306に、許可するIDとパスワードを埋め込ませる。

【0052】処理A-8：生成要求を受けたアクセス受付プログラム生成部301は指示内容に応じたアクセス受付プログラム306を生成し、起動する。

【0053】処理A-9：アクセス受付プログラム生成部301は、要求受付部302に、生成し、起動したアクセス受付プログラムへのアクセス受付アドレスを通知する。アクセス受付アドレスは、本実施の形態では、インターネットで使われるTCP/IPプロトコルのIPアドレスとポート番号とする。

【0054】処理A-10：要求受付部302は、ユーザインターフェイス部303に生成されたIDとパスワードとアクセス受付プログラムのアクセス受付アドレスを通知する。

【0055】処理A-11：通知を受けたユーザインターフェイス部303はIDとパスワードとアクセス受付

プログラムのアクセス受付アドレスをテレビの画面に表示する。

【0056】 こうして、一時アクセス用のIDとパスワードとアクセス受付プログラム306のアクセス受付アドレスを得たユーザは、それらのアクセス情報を、ユーザがアクセスを許可する相手（ここではメンテナンスサービスの担当者）に、何らかの手段、例えば、電話や電子メールなどを使って通知する。

【0057】 ここで、アクセス制御情報保存部（図12の1405参照）に保存されるアクセス制御情報の内容の例を図8に示しておく。

【0058】 次に、図9は、アクセス受付プログラム生成部のフローチャートを示したものであり、以下に処理の流れに沿って説明する。

【0059】 ステップ901：アクセス受付プログラム生成部301は、ユーザから生成要求が来るまで待機する。

【0060】 ステップ902：アクセス受付プログラム生成部301は、生成要求が来るとそれを受け付ける。生成要求には、「アクセス許可内容」と「アクセス許可条件」が含まれる。具体例をあげると、「アクセス許可内容」としては、アクセス先電子機器種別コード、電子機器にアクセスするための、ネットワーク上でのアドレス、使用を許可する操作コマンドの種類など、又、「アクセス許可条件」としては、アクセス許可対象者（誰にアクセス権を与えるか）、アクセスを許可する期間、アクセスを許可するアクセス元アドレス、アクセス回数、指定した電子機器の指定した動作に関連した各種条件（例えば、あるセンサーが反応してから1時間の間だけ、といった条件）などがあろう。

【0061】 ステップ903：生成要求時に得られただけでは情報が足りない場合は、あらかじめ決められた方法で生成に必要な情報、例えば、利用可能な操作コマンドとそのパラメータ、機能情報などを取得する。ここでは、電子機器メーカーが用意したインターネット上の機器情報データベース（図示せず）にアクセスして必要な情報を取得することとする。

【0062】 ステップ904：得られた情報を元にアクセス受付プログラム306のソースコードを生成する。ソースコードのプログラミング言語は特に規定しない。

【0063】 ステップ905：生成されたソースコードを実行形式にコンパイルする。

【0064】 ステップ906：コンパイルの結果生成されたアクセス受付プログラム306を起動する。

【0065】 ステップ907：要求受付部302にアクセス受付アドレスを通知する。

【0066】 以上の、処理の後、エアコンの持ち主であるAさんが、例えば、電子メールや電話などの方法で、メンテナンスサービス業者のBさんに、IDとパスワードとアクセス受付プログラムのアクセス受付アドレス

通知したとして、その後、実際にBさんがAさん宅のエアコンにアクセスするまでの処理の流れを示したものが図10である。以下、図10に沿って説明する。

【0067】 処理B-1：アクセスするユーザ（Bさん）は、Aさんから指定されたアクセス許可期間に入ってから、アクセス装置600のプログラム実行部601（本実施の形態では、パーソナルコンピュータ上のWebブラウザ）を使用し、Aさんに指定されたアクセス受付アドレスを入力する。

【0068】 処理B-2：Webブラウザはアクセス先のアクセス受付プログラム306のアドレスにアクセスする。なお、本実施の形態の場合は、Webブラウザとアクセス受付プログラム306の間でのデータの送受信はWWWサービスで利用されるHTTPプロトコルを利用して行われることとする。

【0069】 処理B-3：アクセス受付プログラム306は、IDとパスワードの入力画面をWebブラウザに送信する。

【0070】 処理B-4：Bさんは、Aさんから通知されたIDとパスワードを入力する。

【0071】 処理B-5：入力されたIDとパスワードをアクセス受付プログラム306に送信する。

【0072】 処理B-6：IDとパスワードを受け取ったアクセス受付プログラム306は、そのIDとパスワードを解析し、アクセス許可内容、及びアクセス許可条件をチェックし、アクセス許可が可能であるか、可能であるとしたりのような内容について操作を許可するのかを判断する。

【0073】 処理B-7：アクセスを許可すると判断した場合は、Webブラウザにエアコンの操作画面を送信する。ここでは、許可されている「保守コマンド」の操作のみが可能であるような画面が生成される。アクセスを許可しない場合は、アクセス拒絶の旨を伝えて通信を切断する。

【0074】 処理B-8：Bさんは、Webブラウザ上に表示されたコマンド操作画面で、エアコンの操作を行う。この例では、「保守コマンド」しかできなくなっているので保守コマンドを実行する。

【0075】 処理B-9：Webブラウザにより、入力されたコマンドはアクセス受付プログラム306に転送される。

【0076】 処理B-10：アクセス受付プログラム306は、保持しているアクセス許可内容、アクセス許可条件をもとにアクセス先（ここではエアコン）へのアクセスを許可してよいか、すなわち、受け取ったコマンドを中継してよいのかチェックを行う。

【0077】 処理B-11：アクセスを許可すると判断した場合は、実際のアクセス先のエアコンにコマンドを転送する。アクセスを許可しない場合は、アクセス権がないとアクセスクライアントプログラム1412

(図12)に伝え、通信を切断する。

【0078】処理B-12:アクセス受付プログラム306は、アクセス先のエアコン(正確にはエアコン上で動作しているサービスプログラム)が返したコマンドに対する応答を受け取る。

【0079】処理B-13:アクセス受付プログラム306は、受け取った応答を、Webブラウザに伝送として転送する。

【0080】処理B-14:応答を受け取ったWebブラウザは、その内容を画面に表示することにより、Bさんはコマンドに対するアクセス対象の応答を得ることが出来る。

【0081】次に、図11に、アクセス受付プログラムの処理のフローチャートを示す。

【0082】ステップ1101:アクセス受付プログラム306は、起動と同時に、外部電子機器ネットワーク308上からのアクセスが来るのを待つ。

【0083】ステップ1102:アクセスがあると、Webブラウザにパスワード入力画面を送信する。

【0084】ステップ1103:Webブラウザで入力されたIDとパスワードを取得する。

【0085】ステップ1104:受け取ったIDとパスワードが正しいかどうか、アクセス受付プログラム306の内部に保持してあるIDとパスワードのデータと照合し、認証を行う。認証に失敗した場合は、アクセスを許可しないことになり、ステップ1107に進む。

【0086】ステップ1105:アクセス受付プログラム306の内部に保持してあるアクセスチケット1413(図12)のアクセス許可内容とアクセス許可条件をチェックし、アクセス許可内容へのアクセスを許可可能かどうかを調べる。アクセスを許可できない場合は、ステップ1107に進む。

【0087】ステップ1106:アクセスが許可されたので、エアコンの操作画面を送信する。

【0088】ステップ1107:アクセス拒絶を相手に伝えて通信を切断する。

【0089】ステップ1108:エアコンの操作のコマンドを受信する。

【0090】ステップ1109:アクセス受付プログラム306の内部に保持しているアクセス許可内容を元に、受信したコマンドがアクセス許可されるかどうかを調べ、許可されない場合は、ステップ1114へ進む。

【0091】ステップ1110:アクセス受付プログラム306の内部に保持しているアクセス許可条件を調べ、受信したコマンドがアクセス許可されるかどうかを調べ、許可されない場合は、ステップ1114へ進む。

【0092】ステップ1111:実際のアクセス先(ここではエアコン)にコマンドを転送する。

【0093】ステップ1112:アクセス先のエアコン(正確にはエアコン上で動作しているサービスプログラム

ム)が返したコマンドに対する応答を受け取る。

【0094】ステップ1113:受け取った応答をアクセスクライアントプログラム1412に伝送として転送する。

【0095】ステップ1114:アクセスを許可しない場合は、アクセス権がないことをアクセスクライアントプログラム1412に伝え、通信を切断する。

【0096】なお、本処理フロー(図11)には記していないが、アクセス許可条件が満たされない状態になった場合(例えば、アクセス許可期間が過ぎた場合など)には、アクセス許可条件が満たされない状態になった旨を相手側に通知し、通信を切断し、アクセス受付プログラムは終了する。

【0097】以下に、本実施の形態の補足を記す。

【0098】まず、アクセス制御装置の各構成要素は、1つの電子機器上に固まって存在する必要はなく、分散オブジェクト技術などを用いてネットワーク上に分散して存在していてもよい。

【0099】又、本実施の形態では、要求受付部は、内部ネットワーク上からの要求を受け付けるような例を挙げたが、外部ネットワーク上からの要求をも受け付けるようにしてもよい。

【0100】又、本実施の形態では、要求受付部は、ユーザ(人)からの要求指示を受け取ったが、電子機器、又はその上で動作しているサービスプログラムが出した要求指示を受け取っても構わない。

【0101】次に、アクセス受付プログラムについてであるが、本実施の形態では、アクセス受付プログラムはアクセス対象機器がエアコンだけであったが、複数のアクセス先へのアクセスを一つのアクセス受付プログラムが受け持っても構わない。

【0102】又、同一のアクセス許可内容に対して、アクセス許可条件で複数のアクセス者からのアクセスを可能にした場合には、一つのアクセス受付プログラムで同時に複数のアクセスを受け付けるようにしても構わない。

【0103】又、本実施の形態ではエアコンの保守操作を例に挙げたが、アクセス受付プログラム経由でやり取りするデータは、コマンドデータだけに限らず、映像、音声、GUI(グラフィカルユーザインターフェイス)データなどの送受信を行ってもよい。

【0104】又、アクセス受付プログラムは、アクセス元とアクセス先との間の通信データの中継をする際に、必要に応じて、通信データに含まれる内容(例えば、アドレスなど)の修正や変換を行ってもよい。

【0105】又、アクセス受付プログラムの生成について、本実施の形態では、ソースコードを生成し、それをコンパイルする方式を用いたが、生成に必要な情報として取得したデータの中に、実行形式のプログラム、又はその一部(バイナリやオブジェクト)が含まれてお

く、その実行形式のデータを修正することによってコンパイルなしでアクセス受付プログラムを生成してもよい。アクセス受付プログラムは、アクセス制御情報のデータと実行形式のプログラムの集合体で、生成に必要な情報として取得したデータの中に、実行形式のプログラムの一部、又は全部が含まれる場合でも、それ単体だけでなく、アクセス制御情報と合わせて初めてアクセス受付プログラムとなる。

【0106】又、複数のアクセス受付プログラムの間で、プログラム部分の一部又は全部が共通化できる場合は、共通化して利用しても構わない。この場合、アクセス受付プログラム実行時にも、複数のアクセス受付プログラムを起動する代わりに、複数のアクセス受付プログラムの間で一つのプログラム部分の一部又は全部に当たる共通部分を共有し、例えば、複数のアクセス受付アドレスに対するアクセス受付を一つのプログラム部分が並列に処理するように実施しても構わない。

【0107】又、アクセス受付プログラムの生成に必要な情報の取得方法については、以下に示す例のように、いくつかの手法が考えられる。

1. アクセス対象電子機器（本実施の形態ではエアコン）に直接アクセスして取得
2. 内部や外部の電子機器ネットワーク上にあらかじめ用意された電子機器情報データベースにアクセスして取得
3. 生成要求時に生成に必要なデータをすべてをユーザから要求時に受け取る

などである。いずれにしても、本発明では、指定されたアクセス条件とアクセス内容に特化したアクセス受付プログラムの生成が可能であればよく、上記のどの方法を用いても効果は同様である。

【0108】又、実際にアクセスする際の処理については、本実施の形態ではユーザ認証（本人であることの認証）をしていないが、例えば、単にIDとパスワードを知っている者ではなく、Bさんだけにアクセスを許可したいような場合は、接続時にユーザ認証を行うようにしてもよい。

【0109】以上のように、本実施の形態では、外部ネットワークからのアクセスを、必要になった時点で、必要なアクセス内容に対してのみ、必要なアクセス許可条件のもとで、セキュリティレベルを下げずに、許可する事が可能である。この結果、ネットワークを利用した有用なサービスを、ユーザのプライバシーやセキュリティを確保しつつ実現することが可能となり、その実用的効果は大きい。

【0110】（第2の実施の形態）次に、本発明の第2の実施の形態について説明する。

【0111】本実施の形態のアクセス制御システムの全体構成は、第1の実施の形態における図1の構成と同じであり、その手順についても図2と同じ手順であるため、それらの説明は省略する。

【0112】次に、本実施の形態における各電子機器装置の構成についてを説明する。

【0113】図12は、本実施の形態でのアクセス制御装置の構成であり、1401は、アクセス受付プログラムを生成するアクセス受付プログラム生成部、1402は、ユーザからのアクセス制御の要求を受け付ける要求受付部、1403は、モニター装置を通してユーザとのやり取りを行うユーザインターフェイス部、1404は、ネットワークを通じての通信を行う通信管理部、1405は、アクセス制御に必要な情報を保存するアクセス制御情報保存部、1406は、アクセスクライアントプログラムやアクセス受付プログラムを保存するプログラム保存部、1407は、アクセス受付プログラムを管理し、起動、停止などを行うアクセス受付プログラム管理部、1408は、アクセスプログラムやアクセスチケットを装置外部に転送するデータ送信部、1409は、アクセスクライアントプログラムを生成するアクセスクライアントプログラム生成部、1410は、アクセスチケットを生成するアクセスチケット生成部、1411は、アクセス受付プログラム生成部によって生成されたアクセス受付プログラム、1412は、アクセスクライアントプログラム生成部によって生成されたアクセスクライアントプログラム、1413は、アクセスチケット生成部によって生成されたアクセスチケットを示している。又、1414は、アクセス許可条件の内容から不要と判断されたアクセス制御情報、アクセス受付プログラム、アクセスクライアントプログラム、アクセスチケットが存在する場合に、それらを削除する削除部である。又、1415は、電子機器を接続した電子機器ネットワークで、本実施の形態では、家庭内のホームネットワークであり、1416は、広域電子機器ネットワークであり、本実施の形態では、インターネットであるとする。

【0114】図13は、本実施の形態で、外部電子機器ネットワークからのアクセス対象となる内部電子機器ネットワークに接続された電子機器の構成図であり、図4の構成と同じである。

【0115】図13において、1501は、電子機器外部からの操作命令を受け付け、実行するサービスプログラム、1502は、電子機器ネットワークを通じての通信を行う通信管理部、を示している。

【0116】図14は、モニター装置の構成図であり、図5の構成と同じである。図14において、1601は、ユーザの操作を受け付け、その結果を表示するユーザインターフェイス部、1602は、電子機器ネットワーク上のサービスを呼び出し、利用するサービス呼出部、1603は、電子機器ネットワークを通じての通信を行う通信管理部、を示している。

【0117】図15は、外部電子機器ネットワークに接続された、内部電子機器ネットワークへアクセスするために使用されるアクセス装置の構成図であり、図6の構成

と同じである。図6において、1701は、プログラムを実行するプログラム実行部、1702は、クライアントアクセスプログラムやアクセスチケットを受信するデータ受信部、1703は、電子機器ネットワークを通じての通信を行う通信管理部、を示している。本実施の形態では、プログラム実行部は、WWWサービスの利用を可能にするWebブラウザであるとする。

【0118】以下、実際の処理の流れを順に説明していく。更に詳細の処理内容の説明が必要な部分については、この説明の後に別途説明する。

【0119】図16は、アクセス受付プログラム生成までの処理の流れを示したものである。縦の線が各構成要素を示し、矢印が通信やデータの流れを示しており、上から下へ処理は流れていくことを示しているものである。以下、図に沿って順に説明していく。

【0120】処理C-1：ホームネットワークのユーザ（その家の住人のAさん）がテレビの画面でリモコンなど操作して、サービス呼び出し部（図14の1602）の操作画面を表示し、操作することにより、アクセス制御装置のユーザインターフェイス部を呼び出し、その操作画面を表示する。

【0121】処理C-2：アクセス制御装置1400（図2）のユーザインターフェイス部1403の操作画面で、アクセス許可内容、アクセス許可条件、生成したアクセスチケットの転送先などを指定する。ここでは例えば、「2010年5月24日12時から14時までの間だけ、エアコンの保守コマンドのみをチケット保持者が実行できるようにする」という内容のアクセス許可内容とアクセス許可条件を指定したのとして説明を進める。

【0122】処理C-3：ユーザインターフェイス部1403はユーザから指定された内容を要求受付部1402に伝達する。これにより、要求受付部1402は、アクセス受付プログラム生成部1401、アクセスクライアントプログラム生成部1409、アクセスチケット生成部1410、の各生成部に生成要求を出す。生成要求の順番は、特にこの図に示した順番でなくても構わない。

【0123】処理C-4：要求受付部1402は、アクセス受付プログラム生成部1401にアクセス受付プログラムの生成要求を出す。

【0124】処理C-5：生成要求を受けたアクセス受付プログラム生成部1401は指示内容に応じたアクセス受付プログラム1411を生成する。

【0125】処理C-6：アクセス受付プログラム生成部1401は、生成したアクセス受付プログラム1411をプログラム保存部1406に保存する。

【0126】処理C-7：アクセス受付プログラム生成部1401は、要求受付部1402に生成したアクセス受付プログラム1411へのアクセス受付アドレスを通知する。アクセス受付アドレスは、本実施の形態では

インターネットで使われるTCP/IPプロトコルのIPアドレスとポート番号とする。

【0127】処理C-8：要求受付部1402は、アクセスクライアントプログラム生成部1409にアクセスクライアントプログラム1412の生成要求を出す。この時に、ユーザに要求されたアクセス許可内容とアクセス許可条件と、生成したアクセス受付プログラム1411へのアクセス受付アドレスを渡す。

【0128】処理C-9：生成要求を受けたアクセスクライアントプログラム生成部1409は指示内容に応じたアクセスクライアントプログラム1412を生成する。

【0129】処理C-10：アクセスクライアントプログラム生成部1409は、生成したアクセスクライアントプログラム1412をプログラム保存部1406に保存する。

【0130】処理C-11：要求受付部1402は、アクセスチケット生成部1410にアクセスチケット1413の生成要求を出す。この時に、ユーザに要求されたアクセス許可内容とアクセス許可条件と、生成したアクセス受付プログラム1411へのアクセス受付アドレスを渡す。

【0131】処理C-12：生成要求を受けたアクセスチケット生成部1410は指示内容に応じたアクセスチケット1413を生成する。

【0132】処理C-13：アクセスチケット生成部1410はデータ送信部1408を使ってユーザから指定された転送先にアクセスチケット1413を転送する。転送先は、ここではユーザインターフェイス部1403とする。本実施の形態では、ここから更にAさんが、届けたい相手、つまり、ここではエアコンのメンテナンスサービス業者（Bさんとする）に転送することとする。なお、その転送方法は本発明の範囲外なので特に限定しないが、ここでは電子メールを用いて暗号化して送信する方法をとることとする。この他にも、例えば、電話回線などの別のネットワークを使って転送してもよい。

【0133】処理C-14：要求受付部1402は新たにアクセス制御要求が来たことをアクセス受付プログラム管理部1407に通知し、その内容を伝える。この時に、ユーザに要求されたアクセス許可内容とアクセス許可条件と、生成したアクセス受付プログラム1411へのアクセス受付アドレスを渡す。

【0134】処理C-15：アクセス受付プログラム管理部1407はアクセス制御情報保存部1405にユーザから要求のあったアクセス制御情報（アクセス内容とアクセス条件）と、生成したアクセス受付プログラム1411へのアクセス受付アドレスを保存し、それと同時に内容にアクセス受付プログラム管理部1407にも保持しておく。

【0135】処理C-16：アクセス制御情報保存部1405

に保存されるアクセス制御情報の内容の例を図17に示しておく。

【0136】又、図18は図17のアクセス制御情報に対応するアクセスチケットに含まれる情報の内容の例を分かりやすいように図にしたものである。

【0137】次に、図19は、アクセス受付プログラム生成部のフローチャートを示したものであり、以下の処理の流れに沿って説明する。

【0138】ステップ2101：アクセス受付プログラム生成部1409は、ユーザから生成要求が来るまで待機する。

【0139】ステップ2102：アクセス受付プログラム生成部1409は、生成要求が来るとそれを受け付ける。生成要求には、「アクセス許可内容」と「アクセス許可条件」が含まれる。具体例をあげると、「アクセス許可内容」としては、アクセス先電子機器種別コード、電子機器にアクセスするための、ネットワーク上でのアドレス、使用を許可する操作コマンドの種類など、又、「アクセス許可条件」としては、アクセス許可対象者（誰にアクセス権を与えるか）、アクセスを許可する期間、アクセスを許可するアクセス元アドレス、アクセス回数、指定した電子機器の指定した動作に関連した各種条件（例えば、あるセンサーが反応してから1時間の間だけ、といった条件）などがある。

【0140】ステップ2103：生成要求時に得られたデータでは情報が足りない場合は、あらかじめ決められた方法で生成に必要な情報、例えば、利用可能な操作コマンドとそのパラメータ、機能情報などを取得する。ここでは、電子機器メーカーが用意したインターネット上の機器情報データベース（図示せず）にアクセスして必要な情報を取得することとする。

【0141】ステップ2104：得られた情報を元にアクセス受付プログラム1411のソースコードを生成する。ソースコードのプログラミング言語は特に規定しない。

【0142】ステップ2105：生成されたソースコードを実行形式にコンパイルする。

【0143】ステップ2106：コンパイルの結果生成された実行形式のファイルをプログラム保存部1406に保存する。

【0144】アクセス受付プログラム1411の処理フローは以上であるが、アクセスクライアントプログラム生成部1491の処理も、生成するコードが異なるだけで、処理の流れは同様である。

【0145】又、アクセスチケット1413の生成に関しても、ソースコード生成とそのコンパイルの代わりに、あらかじめ決められたデータフォーマットでアクセスチケットのデータを生成する点以外は同様の処理の流れである。

【0146】以上示した処理の後、エディタの待ち態

あるAさんが例えば、電子メールなどの方法で、メンテナンスサービス業者のBさんにアクセスチケットを送信したとして、その後、実際にBさんがAさん宅のエコーンにアクセスするまでの処理の流れを以下に説明する。

【0147】ここで、アクセス受付プログラムの起動方法によって、アクセス受付プログラム管理部の動作に以下の二通りの処理フローが考えられる。（それぞれ請求項2と請求項3の実施の例に相当する。）

（1）アクセス要求の受付が可能と判断される期間の間だけ、アクセス受付プログラムを起動しておく。

（2）アクセス要求の受付が可能と判断される期間の間だけ、アクセス受付プログラムの代わりに、アクセス受付プログラム管理部が、アクセス受付プログラムのアクセス受付アドレスへのアクセスを待ち、アクセス発生時に初めて、対応するアクセス受付プログラムを起動し、処理を移行する。

【0148】どちらの場合もユーザから見た場合、操作等に変わりはなく、（2）の方法で実施したアクセス制御装置の方が、処理は若干複雑にはなるが、アクセス制御装置の負荷は軽いのが特長である。

【0149】（1）の場合の処理フローを示したものが図20であり、（2）の場合の処理フローを示したものが図21である。

【0150】以下、まず図20に沿って処理の流れを説明する。

【0151】処理D-1：アクセス受付プログラム管理部1407は、アクセス制御装置1400が起動された時、又は、新たにアクセス制御情報が追加された時に、アクセス制御情報保存部1405に保存したアクセス制御情報を参照することにより、登録されたアクセス制御情報のアクセス許可条件を参照する。

【0152】処理D-2：アクセス受付プログラム管理部1407は、アクセス許可条件から判断してアクセス要求の受付をしてもよい期間になった時点で、プログラム保存部1406から該当するアクセス受付プログラムを取得し、起動する。例えば、本実施の形態では、アクセス許可条件の中にアクセス許可期間が設定されているので、そのアクセス許可期間になった時点で、該当するアクセス受付プログラムを起動する。

【0153】処理D-3：アクセスするユーザ（Bさん）は、Aさんから電話や電子メールなどで指定されるか、あるいは、アクセスチケットの内容を確認する既存のプログラム（図示せず）にアクセスチケットを入力することにより知った「アクセス許可期間」になってから、パーソナルコンピュータ上のチケット処理プログラムにアクセスチケット1413を入力する。ここではチケット処理プログラムは、ある既知のネットワーク上のサーバ（図示せず）からダウンロードする事で取得し、アクセス装置上のプログラム実行部で実行するものとする。

【0154】処理D-4:チケット処理プログラムは入力されたアクセスチケット1413を解析し、アクセス先のアクセス受付プログラム1411のアクセス受付アドレス、アクセス許可内容、アクセス許可条件を取得する。

【0155】処理D-5:チケット処理プログラムはアクセスチケット1413から得られたアクセス受付プログラム1411のアクセス受付アドレスにアクセスし、アクセス受付プログラムと接続し、アクセスチケット1413を転送する。アクセスチケットに暗号鍵が含まれる場合は、その暗号鍵でデータを暗号化して通信を行う。

【0156】処理D-6:アクセスチケット1413を受け取ったアクセス受付プログラム1411は、そのアクセスチケット1413を解析し、アクセス許可内容、アクセス許可条件をチェックする。

【0157】処理D-7:アクセスを許可すると判断した場合は、チケット処理プログラムにアクセスクライアントプログラム1412を送信する。そうでない場合は、アクセス拒絶の旨を伝えて通信を切断する。受信されたアクセスクライアントプログラム1412は、チケット処理プログラムによって起動されることとする。

【0158】処理D-8:Bさんは、アクセスクライアントプログラム1412の操作画面で、エアコンの操作を行う。この例では、「保守コマンド」しかできなくなっているので保守コマンドを実行する。

【0159】処理D-9:アクセスクライアントプログラム1412は、入力されたコマンドをアクセス受付プログラム1411に転送する。アクセスクライアントプログラム1412に暗号鍵が含まれる場合は、その暗号鍵でデータを暗号化して通信を行う。

【0160】処理D-10:アクセス受付プログラム1411は、同プログラム内、あるいはアクセス制御情報保存部1405に保持しているアクセス許可内容、アクセス許可条件をもとに、アクセスクライアントプログラム1412からのアクセスを許可するかどうかの判断を行う。

【0161】処理D-11:アクセスを許可すると判断したならば、実際のアクセス先であるエアコンにコマンドを転送する。アクセス許可しない場合は、アクセス権がない旨をアクセスクライアントプログラム1412に伝え、通信を切断する。

【0162】処理D-12:アクセス受付プログラム1411は、アクセス先のエアコン（正確にはエアコン上で動作しているサービスプログラム）が返したコマンドに対する応答を受け取る。

【0163】処理D-13:アクセス受付プログラム1411は、受け取った応答を、アクセスクライアントプログラム1412に応答として転送する。

【0164】処理D-14:応答を受け取ったアクセス

クライアントプログラム1412が、その内容を画面に表示することにより、Bさんはコマンドに対する応答を得る。

【0165】次に、図21に沿って上記(2)の場合の処理の流れを説明する。

【0166】処理E-1:アクセス受付プログラム管理部1407は、アクセス制御装置1400が起動された時、又は、新たにアクセス制御情報が追加された時に、アクセス制御情報保存部1405に保存したアクセス制御情報を参照する。

【0167】処理E-2:アクセス受付プログラム管理部1407は、アクセス許可条件から判断してアクセス要求の受付をしてもよい期間になった時点で、アクセス制御情報保存部1405から該当するアクセス受付プログラムのアクセス受付アドレスを取得し、そのアドレスへのアクセスを待つ。例えば、本実施の形態では、アクセス許可条件の中にアクセス許可期間が設定されているので、そのアクセス許可期間になった時点で、該当するアクセス受付プログラムのアクセス受付アドレスへのアクセス待ちを開始する。

【0168】処理E-3:アクセスするユーザ(Bさんは、Aさんから電話や電子メールなどで指定されるか、あるいは、アクセスチケットの内容を確認する既存のプログラム(図示せず)にアクセスチケットを入力することにより知った「アクセス許可期間」になってから、パーソナルコンピュータ上のチケット処理プログラムにアクセスチケットを入力する。ここではチケット処理プログラムは、ある既知のネットワーク上のサーバ(図示せず)からダウンロードするなどして取得し、アクセス装置上のプログラム実行部1701(図19参照)で実行するものとする。

【0169】処理E-4:チケット処理プログラムは入力されたアクセスチケット1413を解析し、アクセス先のアクセス受付プログラムのアクセス受付アドレス、アクセス許可内容、アクセス許可条件を取得する。

【0170】処理E-5:チケット処理プログラムはアクセスチケット1413から得られたアクセス受付プログラム1411のアドレスにアクセスする。

【0171】処理E-6:アクセス受付プログラム管理部1407は、プログラム保存部1406からアクセス受付アドレスに該当するアクセス受付プログラムを取得し、起動し、そのアクセス受付プログラム1411に処理を移行する。

【0172】処理E-7:チケット処理プログラムはアクセス受付プログラム1411にアクセスチケット1413を転送する。アクセスチケット1413に暗号鍵が含まれる場合は、その暗号鍵でデータを暗号化して通信を行う。

(以下は図20と同様の処理の流れである)

処理E-8:アクセスチケット1413を受け取ったア

クセス受付プログラム1411は、そのアクセスチケットを解析し、アクセス許可内容、アクセス許可条件をチェックする。

【0173】処理E-9：アクセスを許可すると判断した場合は、チケット処理プログラムにアクセスクライアントプログラム1412を送信する。そうでない場合は、アクセス拒絶の旨を伝えて通信を切断する。受信されたアクセスクライアントプログラム1412は、チケット処理プログラムによって起動されることとする。

【0174】処理E-10：Bさんは、アクセスクライアントプログラム1412の操作画面で、エアコンの操作を行う。この例では、「保守コマンド」しかできなくなっているので保守コマンドを実行する。

【0175】処理E-11：アクセスクライアントプログラム1412は、入力されたコマンドをアクセス受付プログラム1411に転送する。アクセスクライアントプログラム1407に暗号鍵が含まれる場合は、その暗号鍵でデータを暗号化して通信を行う。

【0176】処理E-12：アクセス受付プログラム1411は、同プログラム内、あるいはアクセス制御情報保存部1405に保持しているアクセス許可内容、アクセス許可条件をもとに、アクセスクライアントプログラム1412からのアクセスを許可するかどうかの判断を行う。

【0177】処理E-13：アクセスを許可すると判断したならば、実際のアクセス先であるエアコンにコマンドを転送する。アクセスを許可しない場合は、アクセス権がない旨をアクセスクライアントプログラムに伝え、通信を切断する。

【0178】処理E-14：アクセス受付プログラム1411は、アクセス先のエアコン（正確にはエアコン上で動作しているサービスプログラム）が返したコマンドに対する応答を受け取る。

【0179】処理E-15：アクセス受付プログラム1411は、受け取った応答を、アクセスクライアントプログラム1412に転送する。

【0180】処理E-16：応答を受け取ったアクセスクライアントプログラム1412が、その内容を画面に表示することにより、Bさんはコマンドに対する応答を得る。

【0181】なお、図21で示した、アクセス受付プログラムの代わりにアクセス受付プログラム管理部1407がアクセス受付プログラムのアクセス受付アドレスへのアクセスを待つ場合では、アクセス受付プログラムは一定時間アクセスがない場合は自動的に終了するようにしてもよい。

【0182】又、図20、図21には含まれていないが、あるアクセス受付プログラムについて、アクセス許可条件を満たさない状態になった場合、例えば、本実施の形態では、アクセス受付プログラムのアクセス許可

間が過ぎた場合には、アクセス受付プログラム管理部1407は、そのアクセス受付プログラムが起動している場合は、そのアクセス受付プログラムに対して終了命令を出して終了させ、続いて削除部1414が、不要になったアクセス制御情報保存部1405に保存されているアクセス制御情報、アクセス受付プログラム、アクセスクライアントプログラム、アクセスチケット1413があれば、それらを削除する。

【0183】次に、図22に示したアクセス受付プログラムの処理のフローチャートについて、処理の流れに沿って説明する。

【0184】ステップ2401：アクセス受付プログラム1411は、起動と同時に、外部ネットワーク上のチケット処理プログラム、又はアクセスクライアントプログラムからのアクセスが来るのを待つ。

【0185】ステップ2402：アクセスがあると、それがチケット処理プログラムからのアクセスチケット受付の要求かアクセスクライアントプログラム1412からのアクセスであるかを調べ、アクセスクライアントプログラム1412からのアクセスの場合は、ステップ2409に進む。

【0186】ステップ2403：チケット処理プログラムからのアクセスチケット受付の要求であった場合には、アクセスチケット1413を受け取る。アクセスチケット1413に暗号鍵が含まれる場合は、その暗号鍵でデータを暗号化して通信を行う。

【0187】ステップ2404：受け取ったアクセスチケットが本物であるかの認証を行う。認証の方法はいろいろあるが、例えば、生成時にアクセスチケット生成部1410で内容を暗号化し、その暗号鍵をアクセス制御装置1400で保持しておき、アクセスチケット1413を受け付けの際に、それで復号化出来れば本物であるとする、という方法がある。認証に失敗した場合は、ステップ2408に進む。

【0188】ステップ2405：アクセスチケット1413の中身を解析し、アクセス許可内容とアクセス許可条件を取得する。

【0189】ステップ2406：アクセスチケット1413のアクセス許可内容とアクセス許可条件をチェックし、アクセス許可内容へのアクセスを許可可能かどうかを調べる。

【0190】ステップ2407：許可可能と判断した場合は、アクセスクライアントプログラム1412を転送し、ステップ2401のアクセス待ちに戻る。

【0191】ステップ2408：アクセス拒絶を相手に伝えて通信を切断する。

【0192】ステップ2409：アクセスクライアントプログラム1412からのアクセスの場合は、アクセスクライアントプログラム1412が本物であるかの認証を行う。認証の方法はいろいろあるが、例えば、生成時に

ブ2404で述べた方法と同様に、生成時に内容をアクセスクライアントプログラム生成部で内容を略号化し、その略号鍵をアクセス制御装置1400で保持しておき、アクセスクライアントプログラム1412を受け付けた際には、それで復号化出来れば本物であるとする、という方法がある。

【0193】ステップ2410：アクセスクライアントプログラム1412と接続する。

【0194】ステップ2411：アクセスクライアントプログラム1412からのコマンドを受信する。

【0195】ステップ2412：保持しているアクセス許可内容を元に、受信したコマンドがアクセス許可されるかどうかを調べ、許可されない場合は、ステップ2417へ進む。

【0196】ステップ2413：保持しているアクセス許可条件を調べ、受信したコマンドがアクセス許可されるかどうかを調べ、許可されない場合は、ステップ2417へ進む。

【0197】ステップ2414：実際のアクセス先（ここではエアコン）にコマンドを送信する。

【0198】ステップ2415：アクセス先のエアコン（正確にはエアコン上で動作しているサービスプログラム）が返したアクセスに対する応答を受け取る。

【0199】ステップ2416：受け取った応答をアクセスクライアントプログラム1412に応答として転送する。

【0200】ステップ2417：アクセスを許可しない場合は、アクセス権がないことをアクセスクライアントプログラム1412に伝え、通信を切断する。

【0201】なお、本処理フロー（図2）には記していないが、アクセス許可条件が満たされない状態になった場合（例えば、アクセス許可期間が過ぎた場合など）には、アクセス受付プログラムは、アクセス受付プログラム管理手段からプログラム終了命令の信号を受け、終了する。ただし、もし、ユーザがアクセス中の場合には、アクセス許可条件が満たされない状態になった旨を相手側に通知し、通信を切断した後終了する。

【0202】以下に、本実施の形態の補足事項を記す。

【0203】まず、アクセス制御装置の各構成要素は、1つの電子機器上に固まって存在する必要はなく、分散オブジェクト技術などを用いてネットワーク上に分散して存在していてもよい。

【0204】又、本実施の形態では、要求受付部は、内部ネットワーク上からの要求を受け付けるような例を挙げたが、外部ネットワーク上からの要求をも受け付けるようにしてもよい。

【0205】又、本実施の形態では、要求受付部は、ユーザ（人）からの要求指示を受け取ったが、電子機器、又はその上で動作しているサービスプログラムが出した要求指示を受け取っても構わない。

【0206】次に、アクセス受付プログラムについてであるが、本実施の形態では、アクセス受付プログラムはアクセス対象機器がエアコンだけであったが、複数のアクセス先のアクセスを一つのアクセス受付プログラムが受け持っても構わない。

【0207】又、同一のアクセス許可内容に対して、アクセス許可条件で複数のアクセス者からのアクセスを可能にした場合には、一つのアクセス受付プログラムで同時に複数のアクセスを受け付けるようにしても構わない。

【0208】又、本実施の形態ではエアコンの保守操作を例に挙げたが、アクセス受付プログラム経由でやり取りするデータは、コマンドデータだけに限らず、映像、音声、GUI（グラフィカルユーザーインターフェイス）データなどの送受信を行ってもよい。

【0209】又、アクセス受付プログラムは、アクセス元とアクセス先との間の通信データの中継をする際に、必要に応じて、通信データに含まれる内容（例えば、アドレスなど）の修正や変換を行ってもよい。

【0210】又、アクセス受付プログラムとアクセスクライアントプログラムの生成について、本実施の形態では、ソースコードを生成し、それをコンパイルする方式を用いたが、生成に必要な情報として取得したデータの中に、実行形式のプログラム、又はその一部（ライブラリやオブジェクト）が含まれてもよく、その実行形式のデータを修正することによってコンパイルなしでアクセス受付プログラムを生成してもよい。アクセス受付プログラムとアクセスクライアントプログラムは、共にアクセス制御情報のデータと実行形式のプログラムの集合体であり、生成に必要な情報として取得したデータの中に、実行形式のプログラムの一部、又は全部が含まれる場合でも、それ単体だけではなく、アクセス制御情報と合わせて初めて、それぞれ、アクセス受付プログラム、及びアクセスクライアントプログラムとなる。

【0211】又、複数のアクセス受付プログラムの間で、プログラム部分の一部又は全部が共通化できる場合は、共通化して利用しても構わない。この場合、アクセス受付プログラム実行時にも、複数のアクセス受付プログラムを起動する代わりに、複数のアクセス受付プログラムの間で一つのプログラム部分の一部又は全部に当たる共通部分を共有し、例えば、複数のアクセス受付アドレスに対するアクセス受付を一つのプログラム部分が並列に処理するように実施しても構わない。

【0212】又、アクセス受付プログラム、アクセスクライアントプログラム、及びアクセスチケットの生成に必要な情報の取得方法については、以下に示す例のように、いくつかの手法が考えられる。1. アクセス対象（本実施の形態ではエアコン）に直接アクセスして取得2. 内部や外部の電子機器ネットワーク上にあらかじめ用意された電子機器情報データベースにアクセスして取得3. 本

成要求時に生成に必要なデータをすべてをユーザから要求時に受け取るなどである。いずれにしても、本発明では、指定されたアクセス条件とアクセス内容に特化したアクセス受付プログラム、アクセスクライアントプログラム、及びアクセスチケットの生成が可能であればよく、上記のどの方法を用いても効果は同様である。

【0213】又、実際にアクセスする際の処理については、本実施の形態ではユーザ認証（本人であることの認証）をしていないが、例えば、単にアクセスチケットの保有者というのではなく、Bさんだけにアクセスを許可したいような場合は、接続時にユーザ認証を行うようにしてもよい。

【0214】又、データ受信部を含むアクセス装置（本実施の形態では、パーソナルコンピュータ）は、アクセス時には外部ネットワーク上であるわけであるが、アクセスチケットを受信した時点では内部ネットワーク内に存在してもよい。例えば、内部ネットワーク内でAさんが、携帯型のコンピュータ端末などのデータ受信部を含む電子機器でアクセスチケットを受信し、その電子機器を内部ネットワーク環境の外部に持ち運んで、外部ネットワーク上からアクセスしても構わない。

【0215】又、本実施の形態では、アクセスチケットと引き換えにアクセスクライアントプログラムを得るという処理手順になっているが、アクセスチケットを使わずに最初から直接、アクセスクライアントプログラムを必要な相手に転送し、使用してもよい。この場合でも同様なアクセス制御が可能である。逆に、アクセスクライアントプログラムを使用せずに、アクセスチケットのみを使用してもよい。この場合は、アクセスチケットと引き換えにアクセスクライアントプログラムを得るのではなく、例えば、操作画面が直接アクセス者のアクセス装置のプログラム実行部（例えば、本実施の形態では、Webブラウザ）に送信され、表示されるので、これを通してアクセスする、などの処理が可能である。

【0216】又、アクセス制御に必要な情報（アクセス許可条件、アクセス許可内容など）は、アクセス受付プログラム内部に埋め込み情報として保持しても、アクセス制御情報保存部に保持し、その情報をアクセス受付プログラムの実行時に参照してもよい。

【0217】又、アクセスクライアントプログラムについては、本実施の形態では、Webブラウザ上で動くプログラムであるとしても構わず、必ずしもWebブラウザ上で動くものでなくても構わない。又、アクセスクライアントプログラムは、GUI（グラフィカルユーザインターフェイス）や音声入力などの様々なユーザインターフェイスを持ちうる。

【0218】又、アクセスチケットのフォーマットとデータ形式については、アクセスチケットを扱うプログラム同士が互いにその内容を正しく読み取り、処理できさえすれば、たまたまであって構わない。

【0219】又、アクセスチケットは生成時に全体又は一部を暗号化されていても構わない。

【0220】又、本実施の形態では最初にチケット処理プログラムからアクセスする先はアクセス受付プログラムとしたが、別途、アクセスチケットを受け取り、認証を行い、対応するアクセスクライアントプログラムを渡すプログラムをアクセス制御装置などで動作させておいても構わない。

【0221】以上のように、本実施の形態では、外部ネットワークからのアクセスを、必要になった時点で、必要なアクセス内容に対してのみ、必要なアクセス許可条件のもとで、セキュリティレベルを下げずに、許可する事が可能である。又、外部ネットワークからのアクセスを簡単で分かりやすい操作で実行可能である。この結果、ネットワークを利用した有用なサービスを、ユーザのプライバシーやセキュリティを確保しつつ、簡単な操作で実現することが可能となり、その実用的効果は大きい。

【0222】

【発明の効果】以上のように、本発明によれば、動的に生成されるアクセス受付プログラムにより、外部ネットワークからのアクセスを、必要になった時点で、必要なアクセス内容に対してのみ、必要なアクセス許可条件のもとで、セキュリティレベルを下げずに、許可する事を可能とする柔軟なアクセス制御が実現可能となる。

【0223】又、アクセス許可条件から判断してアクセス要求の受付をしてもよい期間の間だけ、アクセス受付プログラムを起動しておくことを可能とするアクセス受付プログラム管理手段により、それ以外の期間では全くアクセス不能にすることが可能となり、セキュリティを向上させることが可能となる。

【0224】又、アクセス許可条件から判断してアクセス要求の受付をしてもよい期間の間だけ、アクセス受付プログラムの代わりにアクセス受付プログラムのアクセス受付アドレスへのアクセスを待ち、アクセス発生時に初めて、対応するアクセス受付プログラムを起動し、そのアクセス受付プログラムに処理を移行するアクセス受付プログラム管理手段により、アクセス要求の受付をしてもよい期間の間ずっと、アクセス受付プログラムを起動しておく必要がなくなり、プログラムを動作させる電子機器の使用する記憶容量や実行する計算処理などを軽減することが可能となる。

【0225】又、アクセスクライアントプログラムを動的に生成し、これを用いることにより、アクセスクライアントプログラムを使用してのアクセス以外は許可しないようにすることや、使用を許可した機能以外は操作できないようにすることが可能となり、セキュリティが向上する。更に、アクセスクライアントプログラムによって、アクセス受付プログラムとの間の独自のアクセスプロトコルを利用者が意識することなく、簡単にアクセス

することが可能となる。更に又、アクセスクライアントプログラムにGUI（グラフィカルユーザインターフェイス）を持たせることにより、利用者がアクセスに必要な操作を簡単に行うことを可能とする。又、アクセスチケットを動的に生成し使用することにより、アクセスチケットがない場合にはアクセスを許可しないようにすることが可能となり、セキュリティが向上する。又、アクセスチケットは、アクセスクライアントプログラムと比較するとデータ容量が大変小さいため、携帯用の電子機器に格納して持ち運ぶ場合などには、アクセスクライアントプログラムを格納する場合よりも、小さな記憶領域しか必要とせず、又、ネットワークを介しての転送時間も短くてすむという効果が得られる。

【0226】又、アクセスクライアントプログラムやアクセスチケットに暗号鍵を含ませることにより、第三者に盗聴や改竄をされない安全な通信を、複雑な暗号鍵交換の仕組みなしで簡単に行うことが可能になる。

【0227】又、アクセス許可条件の内容から不要と判断されたアクセス制御情報、アクセス受付プログラム、アクセスクライアントプログラム、アクセスチケットが存在する場合に、それらを削除する削除手段により、不要となったプログラムやデータが、いつまでも存在し続けることを防ぐことが可能となる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態におけるシステムの全体構成を表す概略ブロック図

【図2】第1の実施の形態における最終的なアクセスの流れを示す概念図

【図3】第1の実施の形態におけるアクセス制御装置の機能的構成を示すブロック図

【図4】第1の実施の形態におけるアクセス対象となる電子機器の機能的構成を示すブロック図

【図5】第1の実施の形態におけるモニター装置の機能的構成を示すブロック図

【図6】第1の実施の形態におけるアクセス装置の機能的構成を示すブロック図

【図7】第1の実施の形態におけるアクセス受付プログラム生成までの処理手順を示したシーケンス図

【図8】第1の実施の形態におけるアクセス受付プログラムが保持しているアクセス制御情報の内容の例を示した図

【図9】第1の実施の形態におけるアクセス受付プログラム生成部の処理を示したフロー図

【図10】第1の実施の形態におけるユーザからのアクセスの処理手順を示したシーケンス図

【図11】第1の実施の形態におけるアクセス受付プログラムの処理を示したフロー図

【図12】第2の実施の形態におけるアクセス制御装置の機能的構成を示すブロック図

【図13】第2の実施の形態におけるアクセス対象となる

電子機器の機能的構成を示すブロック図

【図14】第2の実施の形態におけるモニター装置の機能的構成を示すブロック図

【図15】第2の実施の形態におけるアクセス装置の機能的構成を示すブロック図

【図16】第2の実施の形態におけるアクセス受付プログラム、アクセスクライアントプログラム、アクセスチケットが生成までの処理手順を示したシーケンス図

【図17】第2の実施の形態におけるアクセス受付プログラムが保持しているアクセス制御情報の内容の例を示した図

【図18】第2の実施の形態におけるアクセスチケットが保持している情報の内容の例を示した図

【図19】第2の実施の形態におけるアクセス受付プログラム生成部の処理を示したフロー図

【図20】第2の実施の形態におけるユーザからのアクセスの処理手順を示したシーケンス図

【図21】第2の実施の形態におけるユーザからのアクセスの処理手順を示したシーケンス図

【図22】第2の実施の形態におけるアクセス受付プログラムの処理を示したフロー図

【図23】従来の技術におけるアクセス制御装置の機能的構成を示すブロック図

【符号の説明】

101 アクセス制御装置

102 モニター装置

103 アクセス対象となる電子機器

104 内部電子機器ネットワーク

105 外部電子機器ネットワーク

106 アクセス装置

300、1400 アクセス制御装置

301、1401 アクセス受付プログラム生成部

302、1402 要求受付部

303、1403 ユーザインターフェイス部

304、1404 通信管理部

305、1411 アクセス受付プログラム

306 ID生成部

307、1415 内部電子機器ネットワーク

308、1416 外部電子機器ネットワーク

1405、アクセス制御情報保存部

1406、プログラム保存部

1407、アクセス受付プログラム管理部

1408、データ送信部

1409、アクセスクライアントプログラム生成部

1410、アクセスチケット生成部

1412、アクセスクライアントプログラム

1413、アクセスチケット

1414、削除部

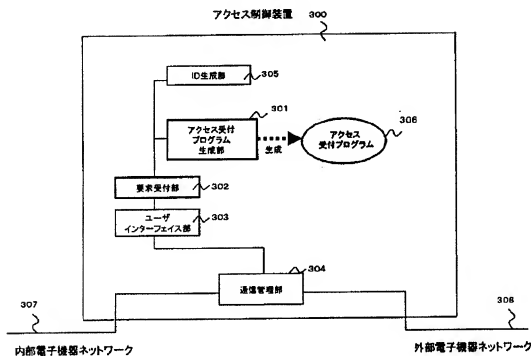
401、1501 サービスプログラム

402、1502 通信制御部

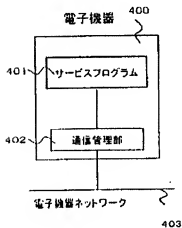
501、1601 ユーザインターフェイス部
 502、1602 サービス呼出部
 503、1603 通信管理部
 601、1701 プログラム実行部
 602、1703 通信管理部
 1702 データ受信部
 2500 従来のアクセス制御装置

2501 要求受付部
 2502 アクセス制御情報保存部
 2503 アクセス 受付プログラム
 2504 通信管理部
 2505 計算機ネットワークネットワーク
 2506 異なる管理下にある計算機ネットワーク

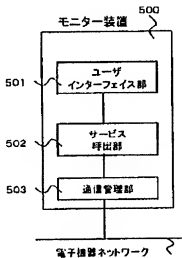
【図3】



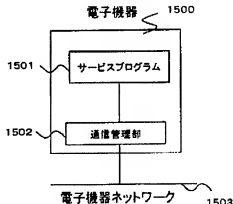
【図4】

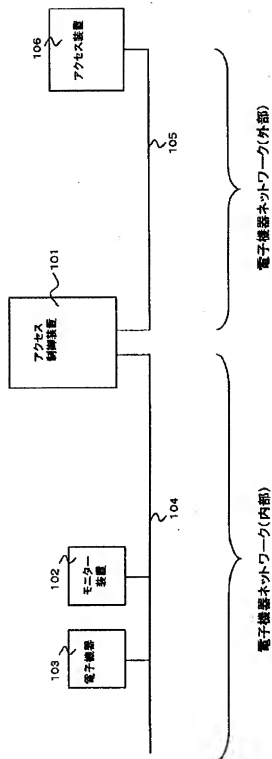


【図5】



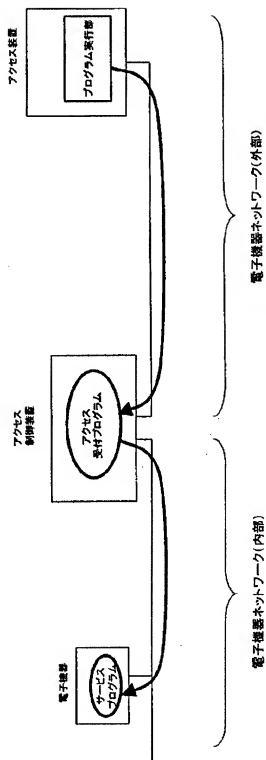
【図13】



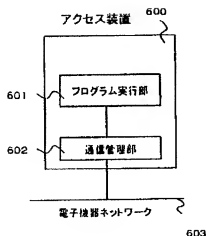


【図 1】

【図2】



【図6】



【図18】

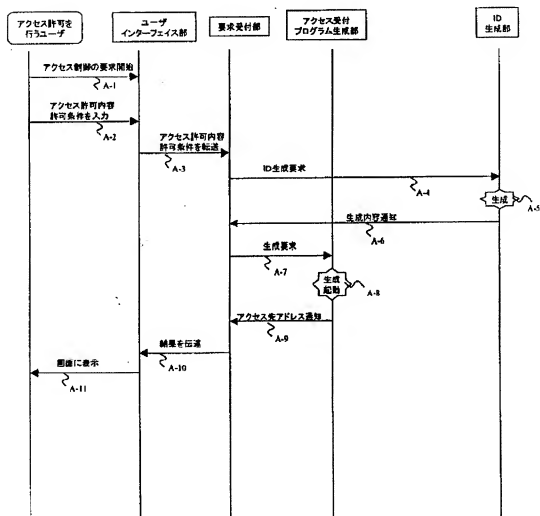
・アクセス許可条件
 アクセス許可対象者: チケット保有者
 有効期間: 2010年05月24日 12:00-14:00

・アクセス許可内容
 アクセス許可対象機種: エアコン(型番ABC-0553)
 アクセス許可機能: 「保守コマンド」のみ
 アクセス先アドレス: 123.456.789.100:1654

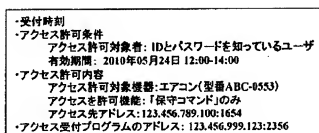
・アクセス受付プログラムのアドレス: 123.456.999.123:2356

・通信時に使う暗号鍵データ
 ・チケットを暗号化した暗号鍵データ

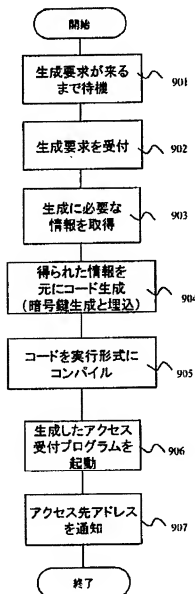
【図7】



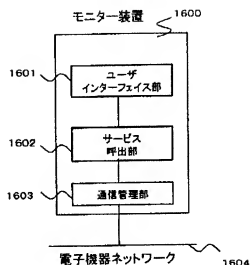
【図 8】



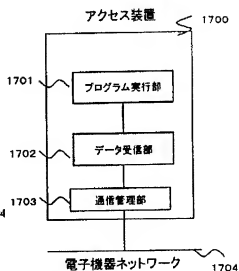
【図 9】



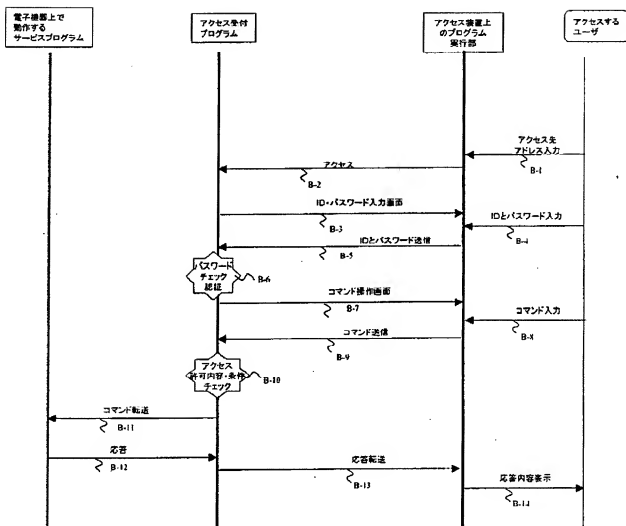
【図 14】



【図 15】

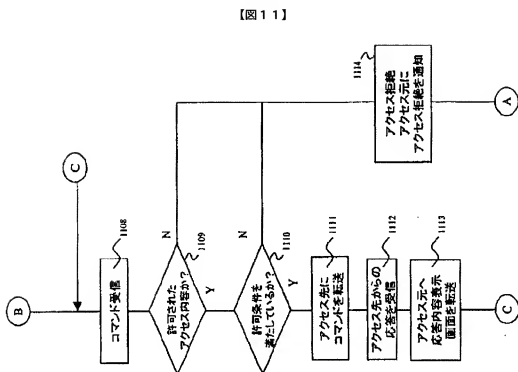
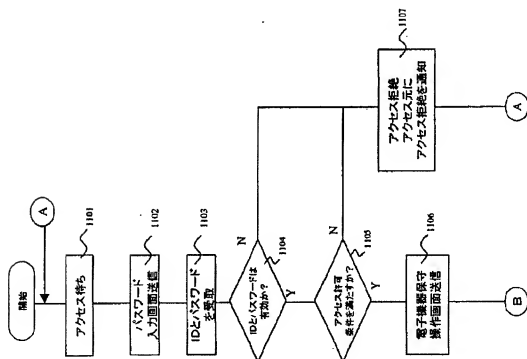


【図 10】



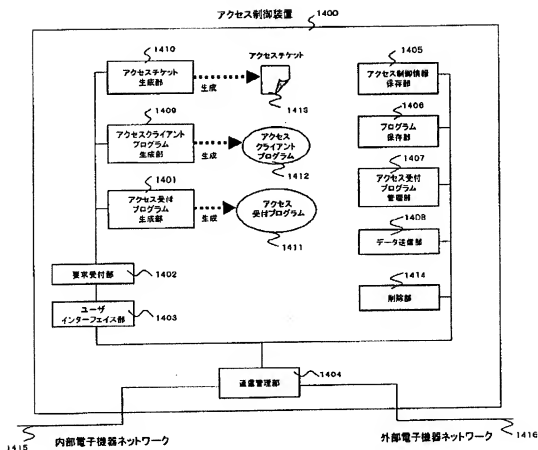
【図 17】

- ・発行時刻
- ・アクセス許可条件
 - アクセス許可対象者: チケット保有者
 - 有効期間: 2010年05月24日 12:00-14:00
- ・アクセス許可内容
 - アクセス許可対象機器: エアコン(型番ABC-0553)
 - アクセスを許可機能: 「保守コマンド」のみ
 - アクセス先アドレス: 123.456.789.100:1654
- ・アクセス受付プログラムのアドレス: 123.456.999.123:1356
- ・通信時に使う暗号鍵データ
- ・チケットを暗号化した暗号鍵データ

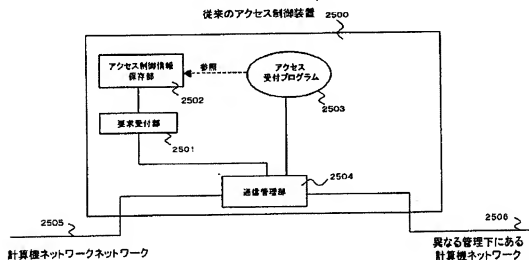


【図11】

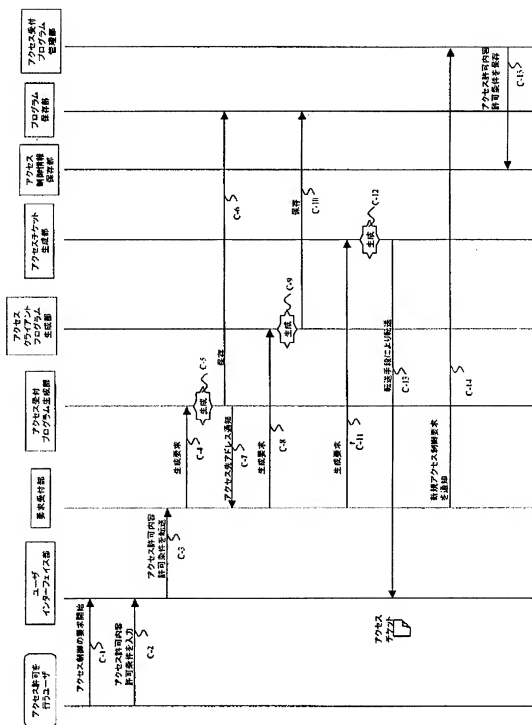
【図12】



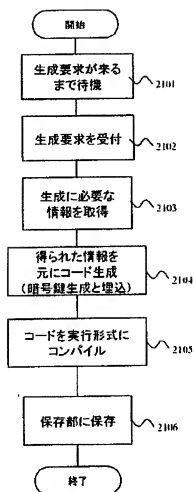
【図23】



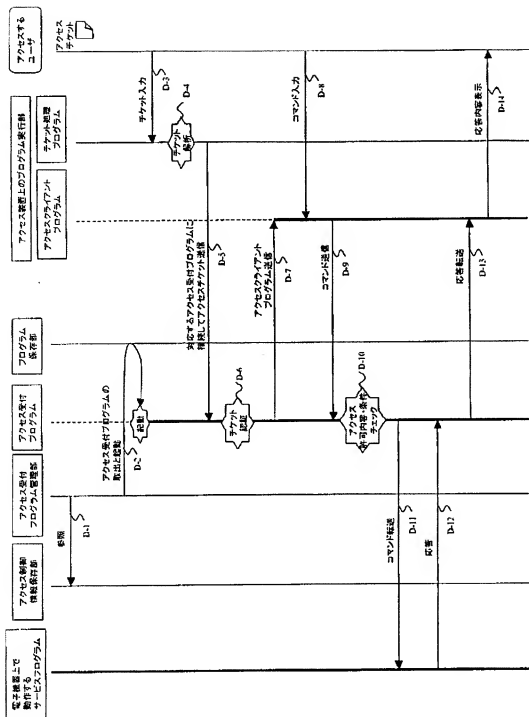
【図 16】



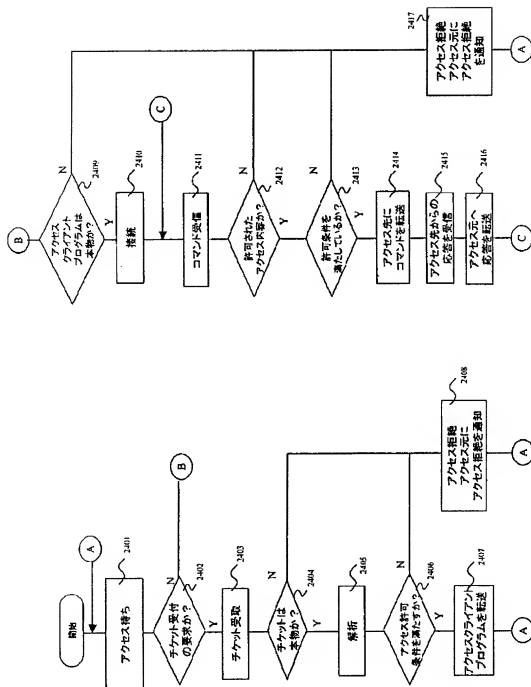
【図19】



[図 20]



【図22】



フロントページの続き

(72)発明者 石川 晃

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 日野 哲也

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 上田 真臣

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

Fターム(参考) 5B085 AE04

5J104 AA07 KA01 KA02 NA05 PA07

5K030 GA15 HB19 HC14 HD01 LD19

5K033 AA08 BA01 DA05

9A001 BB04 CC03 LL03